Inside the ControlGuard CSS Technology

Device Control and Data Loss Prevention

Contents

Summary for IT Administrators	3
What is ControlGuard CSS	5
Network Topology	7
Add-Ons	10
Network Transactions	11
Capacity and Performance of the CSS	13
Configuration & Defining Policies	16
Competitive Edge	18
Summary	20

Summary for IT Administrators

Many years ago, users' only access to company data occurred through dumb terminals to a mainframe. The data resided safely in the data center, and the only way it might physically leave that data center was on reel-to-reel tape or large, heavy hard drives. By contrast, today's users have multiple access points to company data—for example, USB drives, floppy drives, and even burnable CD/DVD drives. Dishonest employees can easily use these points of access to steal sensitive data. If you've considered blasting your users' USB ports with hot glue, you aren't alone. ControlGuard offers elegant solution available to you - Central Security Suite (CSS) will help you take back control of all those vulnerable access points.

Central Security Suite (CSS) requires a next-next installation. After the installation complete, all you need to do is to double- click the ControlGuard Administration Console desktop icon and the software will present you with logon dialog box. The Installation Guide can give you the initial username or password that you need to log on. You can easily change the password from within the administration console. The first time you start the console, a wizard walks you through the configuration process. The User Manual also provides a nice workflow that shows you how to get everything up and running.

The first step in the wizard is to set up directory collaboration with Endpoint Access Manager. The product supports Windows Server 2003 AD, NT domains, Workgroups and Novell eDirectories.

The next step is to add the computers to which you want to apply the settings. If you have your computers segregated into OUs, this step will be simple. For example, if your OU structure contains two OUs called Managers and Ops Floor beneath All Computers, it would be easy to deploy the policies to just those two separate OUs and not to the other servers or domain controllers (DCs).

Central Security Suite (CSS) uses a certificate to ensure that the server and client are communicating with the correct machines. The certificate has to live in the \system32 folder under C:\windows on each client machine. You can copy the certificate manually or use the included MSI Updater to insert the certificate into the MSI installation file. Adding the certificate is simple. If you want, you can also update the .msi file with some initial policies. Doing so helps ensure that all your new PCs are secured as soon as their computer accounts are added to the domain.

Before you can send out a policy to secure endpoints, you need to install the agent onto each PC. The typical methods are available (i.e., setup.exe file, batch script, Group Policy), but what sets Central Security Suite apart is its "on-the-fly distribution". This feature installs the client onto all network computers almost immediately. After you start the Central Security Suite AD Synchronization service, you can set it to synchronize with AD every x minutes. Now, every time a computer is added to AD, the ControlGuard Central Security Suite Service is automatically installed onto the new machine. This method is totally hands-off for the administrator. You have enough to worry about without having to manage the installation of the Central Security Suite client!

The final step is to create Access Control Lists (ACLs) that define which devices can and can't be used on a computer. You can call your first ACL total lockdown and proceeded to lock everything - removable storage, iPods, floppy drives, Bluetooth ports, WiFi adapters, Smartphons, printer ports and more.

When you will login as a normal user on the PC, you will immediately denied access to your USB thumb drive.

After you've secured your network's endpoints, you'll probably want to generate a report either for auditing purposes or for confirmation that you've set everything up correctly. Central Security Suite offers extremely detailed reports via a Web page (For that reason, IIS is required during the initial installation).

What is ControlGuard CSS?

The ControlGuard CSS product family provides policy based solution for monitoring, controlling and securing portable devices, USB ports, peripherals and a host of other security holes that are often standard features on computers of a network. It addresses security issues not handled by traditional security measures and allows IT professionals to implement security over corporate computers, laptops, portable devices and files that leave the trusted network.

The CSS provides policy based monitoring, locking, logging, alerts and actions for securing endpoints and portable devices. Additional functionality gives you complete visibility and control over the transfer of confidential information to removable storage devices and media.

Highlighted features include the ability to keep mirrored copies of transferred data and the support and enforcement of “encryption only” copying policies. This provides automated assurance of employee compliance to file rights management programs.

What can you do with ControlGuard CSS?

You can deploy the ControlGuard CSS to correct deficiencies in an IT security plan that leave endpoints unmonitored, unregulated, exposed and exploitable to abuses as well as to help protect the company against data loss and everyday mistakes made by employees. The CSS can be deployed by IT security to enforce encryption policies as part of regulatory compliance.

With the CSS you can authenticate, monitor, audit, intercede, regulate, control, block, shadow and explore each of the following:

1. **Authorized and Unauthorized User Behaviour**
   The CSS allows the creation of custom policies that allow security to take control and see what is going on in these areas where employees can operate under the radar of traditional security.

2. **Authorized and Unauthorized Endpoints – ports, peripherals and connections**
   The CSS allows audit and control I/O use and abuse as well as detection of attempts by unauthorized devices and connections to access the system through ports, peripherals and wireless interfaces.

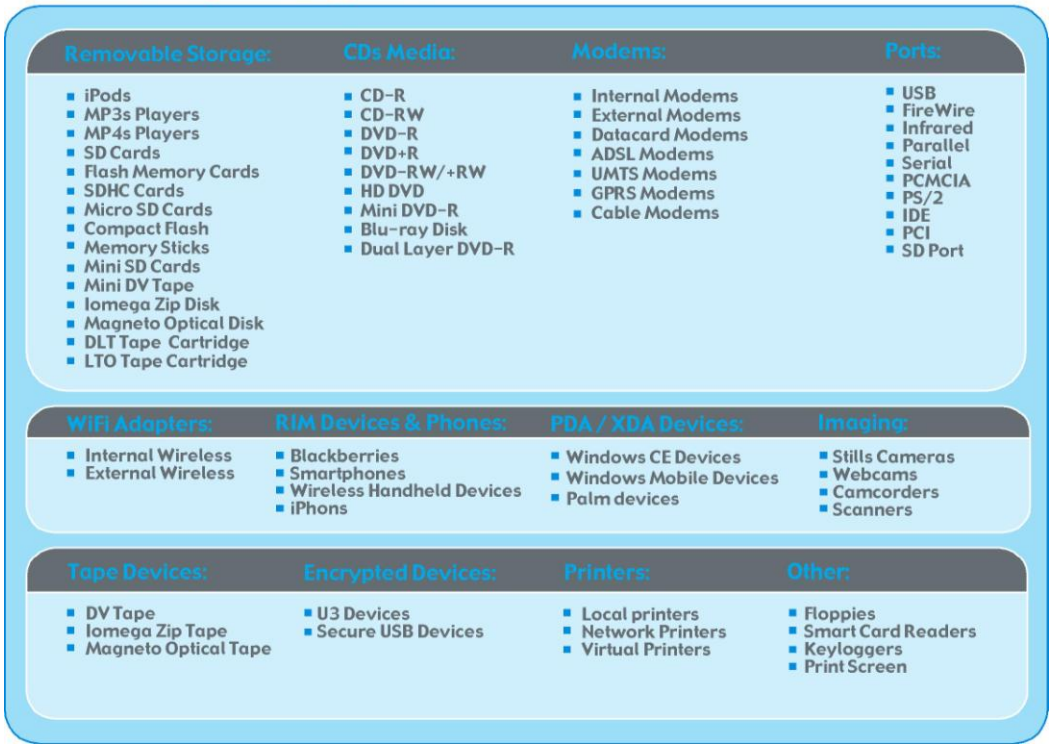
3. **Authorized and Unauthorized Connected Portable Devices and Media Storage Devices**
   With the CSS features you can detect and manage devices such as USB drives, iPods, Bluetooth devices, recordable CDs and DVDs, PDAs, Smartphone devices, Wireless adapters, etc.

With ControlGuard CSS you can add or change access rights without needing to reboot the computer and at the same time to control and monitor all activities from a central location.

Using ControlGuard CSS you can:

- Define user/group based permissions on all/specific machines
- Prevent the use of unknown or unauthorized devices and media
- Identify and authorize only specific device types within a class
- Create a temporary device access and scheduled access for a predefined time
- Restrict the type of files that are copied to device
- Restrict the amount of data copied to a device
- Define what data can and cannot be copied onto allowed devices
- Block or approve specific media as needed (e.g DVDs/CDs/Floppies/SD Cards)
- Log all transactions and mirror files (for shadowing or backup copies) for each event of data written to external devices or specific authorized devices
- Enforce specific users/user groups to encrypt their removable devices
- Enforce encryption to media with the powerful AES algorithm

Supported Devices and Endpoints



Network Topology

The CSS solution is network friendly and uses a three-tiered architecture that is designed to minimize policy-checking traffic. This feature is control by the CSS Agent from the client computer itself and is transparent to the user.

The software application works through distributed agents that communicate with the CSS centralized servers. The design of the CSS Agents ensures that security policies are enforced by the agents whether or not the network can be reached.

The system uses the following components:

- Management Console
- Management Server
- CSS Agent
- Database

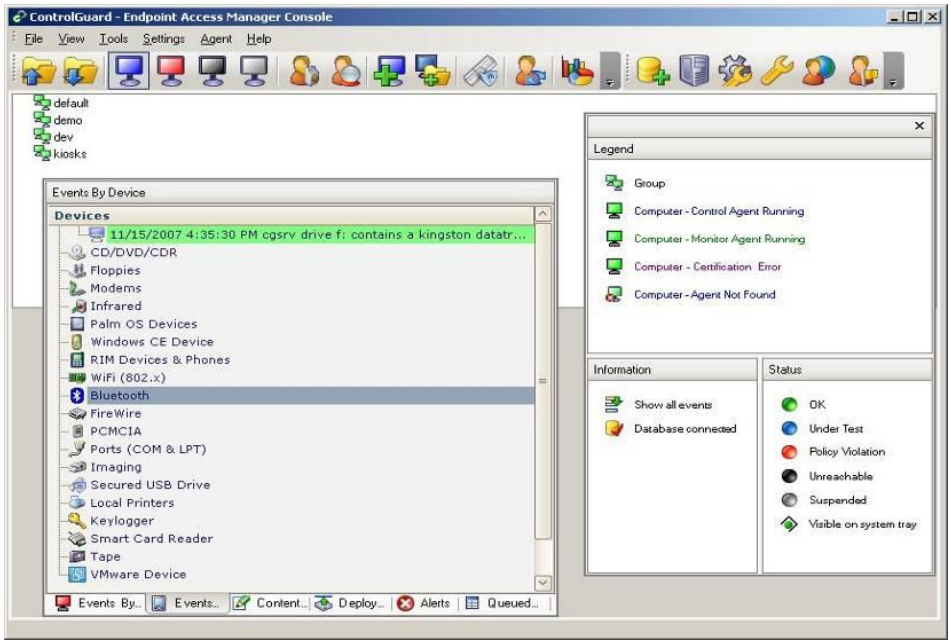
Management Console

The management console provides a heads-up command and control center thin client that allows the IT security administrator to deploy, configure, investigate, monitor, block and authorize users, computers and devices as well as view logs and events. The system supports one or more management consoles and the permissions a user of the console are defined by the user group of the console.

The user groups of the console are:

- Viewer – allows the user to view and read the console data without being able to modify it.
- Policy Manager – allows a user or a user group to define ACLs. The ACL's defined by a policy manager can be applied only to the users and computer groups assigned to him.
- Admin – grants the user administrator permissions, i.e. the ability to access and modify console data.

The following image shows the Management Console main window:



The management console provides ease-of-use and flexible management options. It has a Network Map View providing a network view of all endpoint in the organization. Nodes in the interface are represented with icons that give a color indication of the status of each. For example and icon would show a red agent icon if an agent is not available.
In addition to being an easy-to-use console for managing and gaining oversight of the network and devices, it also provides a command center for assigning access permissions to approved media and devices.

The Central Security Suite enables you to create and assign access permission using a variety approaches, layered positive and negative security policies and at a great number of levels which are discussed further in the Policy Granularity section of this paper.

Management Server

The management server is the core application and clearing house for the Management Console thin clients as well as the event engine and manager of network transactions to and from the Agents that are online.

The management server processes and handles the commands issued by the Management Console clients. It also contains the Audit Logger that keeps track of all changes that users of the Management Console make. This allows security to research, troubleshoot and monitor changes in security configurations that are of interest.

CSS Agent

The CSS Agent runs on the client and enforces the active security policy and logs events and issues security alerts.

The Agent monitors and enforces the security policy whether the computer is connected online, offline or via VPN. In other words, regardless of where the computer is or what it connects to, the CSS Agent maintains its robust security policies at all times. For example, a laptop that is unplugged from the network and is being used in a coffee shop is still being protected.

When online the Agent communicates with the Management console and transmits events and log information to be recorded in the database and for event responses and alerts. Additionally, if the Agent is configured to shadow any of the use on the client, it will transmit this information over the network to be recorded. Note that all transmissions from the Agent to the Management Server and centralized engines of the CSS are encrypted in order to prevent sniffing of the transmitted packets.

When offline, the Agent enforces the ACL policies and controls, monitors, and alerts the user. The log files are protected to prevent the hacker or abuse from being covered up by erasing the log. Events are stored in a vault directory and are maintained in files that are partitioned into bandwidth manageable files that will be transmitted once the computer is back online on the network.

Due to bandwidth limitations, if the computer is using VPN, wireless, cellular, or offline, historical events will not be transmitted. Only when the computer is online, will events transmit.

The Agent provides extensive anti-tampering and security measures and cannot be stopped by the user via the Task Manager. This robust interdependence mechanism means that the user or a hacker is deterred from hacking the security. If the system is attempted to be disabled by a user the incident is logged into the vault and reported. The endpoints are put on automatic lockdown. Using methods similar to a ‘honey pot” hackers will not know whether they are achieving their goals or being delayed.

Because the Agent runs in the kerning before the Operating system or user login, it is more robust and less exposed. It also has access to memory and hardware that user processes and application do not have. If the Agent is tampered with during boot up, the anti-tampering mechanism logs the events into a vault and blocks the ports and devices from access. As this represents a severe form of hacking and likely indicates the machine has been compromised or stolen, the escalated lock down requires contacting ControlGuard to restore the machine.
This operation in the kerning before the OS loads, means the CSS can prevent exploitation of endpoints such as USB hacking that can compromise a machine even when a user is not even logged in. The Agent deploys a security policy before the OS loads.

Additionally the CSS agent can have policy changes effected in real-time. Unlike competitive security solutions that require reboot or cannot stop a user from an action such as using a modem. Once the user has started, the Agent of the CSS can head off abuses in real-time. If a security administrator sees and abuse, they can step in and stop it and the use of a device without waiting till the endpoint is free again. In other words, if a modem is downloading files from the secure zone, competitive solutions must wait till the download is complete and the modem is free again in order to apply changes in a policy. With the CSS this is not the case. The CSS would give instant control to the administrator to stop the download and take control of the modem.

The anti-tampering technology of the CSS Agent is based on a Filter Driver which runs on Kernel Mode. This secure and robust Filter Driver of the CSS Agent employs 14 anti-tampering mechanisms, five of which are hardcore tactical response measure should someone attempt to tamper with or disable the CSS agent.

Database

The database is used to store the configurations and information for the CSS. Although the CSS comes with a redistributable copy of MSDE database, the CSS is most commonly interfaced with the database of the company.

Add-Ons

Add-ons plug-in applications that offer additional productivity and interface features that increase the functionality of the CSS.

Rights Management – Office Document Management

ControlGuard has already acquired and slated the release of the ControlGuard ORM product as well as another encryption and rights management waiting in the wings which will furthering expand ControlGuard's offering. Stay posted on the upcoming Disk Encryption product that will include encryption policies on DVD & CD usage.

Messaging Server

The Messaging server is a plug-in for the Management Console that allows the extension of the notifications from the Agent as well as communication with the agents by the user of the management console.

The extension of the notifications adds a powerful tool for IT professionals by allowing them to not only interact with Users and Agents but also allows the integration of the CSS with third party security information center software. The following is a list of the additional notification features of the Messaging Console add-on.

- **Email**
  Send notifications to email recipients via MS exchange or MS Outlook
- **SNMP**
  Send notifications via SNMP messages
- **Popup – messages**
  Issue popup messages via communication with the ControlGuard agent on the clients.
- **Third Party Security Information Centers**
  Forewords notification to IT security software that consolidates security alerts from various security applications running on the network. For example CA Audit (Computer Associates Audit Program)-eTrust Audit

ControlGuard's Messaging Server provides the following features:

- Correlation: it can connect and integrate the system to any SIM/SOC solution (SIM=security information management; SOC=security operation center) and to 3rd party security and help-desk platform.
- Aggregation: it collects all the events and notifications from the CSS database and enables the sending of alerts to emails, SOC/SIM…
- Escalation: enables user interaction and interdiction to alerts based on the information urgency.

This server allows additional possibilities for monitoring the system, collecting information (general events, forensic events, and content events) and filtering the information according to your needs.

System information is kept in database tables. By defining notification properties (such as message destination and structure), you can be notified whenever database tables are updated with new entries. The messaging

application sends a separate notification for each entry that matches the defined rules.

Live Update

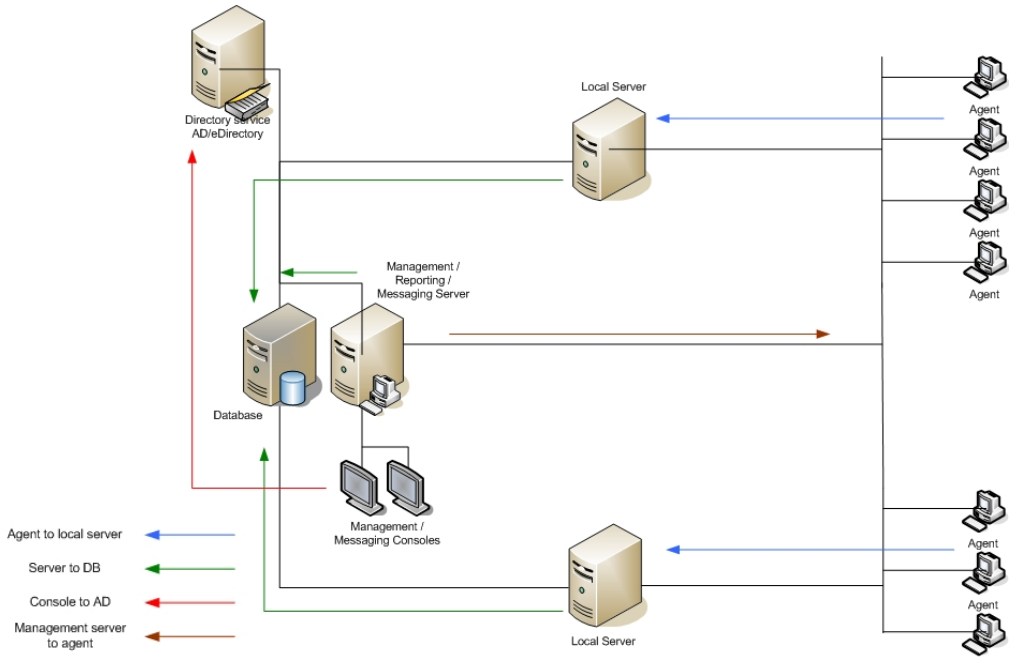
This add-on allows the management of updates and software versions across the network. ControlGuard's Live Update can easily get details on Agents on the network and their current versions as well as providing a centralized console for simultaneously updating all or only specified Agents on the network. The Management Server tracks which agent is deployed on which endpoint. When an update is available to the agent software, the appropriate files are sent to the endpoints based on their current agent version.

Included with the update functionality is a rollback feature that allows the administrator to go back to the previous installed version.

Network Transactions

The network transaction among the Agents, the Management Console and the Management Server are encrypted to prevent sniffing and interception of the information within the network packets. The communication protocol encrypts the data and identifies the source.

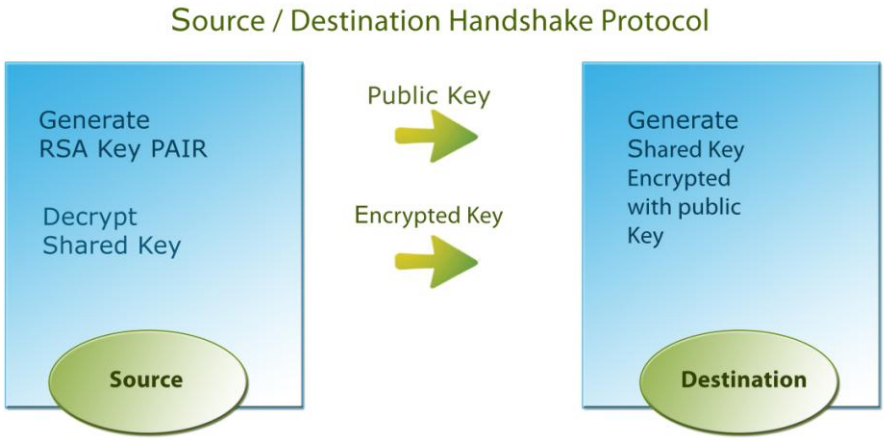
The following diagram shows the communication legs that occur over the network. It is important that this communication is supported unhindered by firewalls.



Network Settings and Protocols

The Management Server communicates with CSS agents and with the Management Console using HTTP protocol over an SSL connection (the communication ports can be configured as needed). CSS agent initiates communication and registers with the server as soon as the endpoint boots and communicates its status and other housekeeping.

Additional communications are sent depending on the agent policy (ACL) configurations, file shadowing and commands issued by the Management Console and Add-ons.



The communication used for encryption and secure connections uses keys for encryption and certificates and works as follows.

The source dynamically generates a key pair and sends the public key to the destination. The destination then dynamically creates a symmetric key, encrypts it with the source's public key, and sends the encrypted key back to the source. The source can now use his private key to decrypt the symmetric key; both ends have the same symmetric key.

Once both ends have the same symmetric key, all data exchanged between them is encrypted using a symmetric encryption.

All messages contain an organizational certificate created when the Management Server is installed. This allows the message recipient to identify the source of the message and act accordingly for example: when an agent receives a message, it checks the message source and if the source is not its corresponding Management server, the message is ignored.

Capacity and Performance of the CSS

The CSS enterprise edition provides a load-balancing feature which allows large systems to manage the traffic from numerous Agents. It should be noted that the CSS works with routers and load balancers, however the feature of the CSS provides alternate Management Servers load balancing feature.

This feature distributes the load across multiple servers for reliable and high-volume output. Highly configurable workflow design allows you to dedicate servers to specialized tasks. Distributed control across servers ensures that if any machine goes down, the system automatically recovers and keeps running.

Central Security Suite enables you to install several servers for load balancing. The first server installed is automatically promoted to a management server. If the management server does not respond, you can promote a different server.

The order of the installed servers on the list determines the order set in the agent's registry during installation. The agents scan the servers' list for an idle server according to the order they are assigned. It is recommended to set the servers order so that the management server is the last server on the list to enable load balancing and to minimize response time.

ControlGuard Central Security Suite can be deployed using one of the following configurations:

Capacity Strategy Type	Number of Endpoints
Single Server Configuration	Up to 12,000 endpoints
Cluster Server Configuration	Above 12,000 endpoints or for High Performance/High Availability/Load Balancing

Scalability

The CSS comes in two versions each providing considerable flexibility. The Enterprise version provides additional scalability features beyond those of the SMB edition. These features provide specialization capabilities and load balancing that assures robust operation optimized handling of traffic and communication. This includes:

- **Scalability**
  Supporting an unlimited number of Agents and endpoints
- **Load Balancing**
  Management server rollover assures that if one server is busy or unavailable that an alternate server will handle the overflow.

- **High Availability**
  Because traffic and server loads are managed the system assures high availability.
- **Fault Tolerance**
  The design of the system provides robust agents that maintain logs and alerts even when the network is down. The system assures that if one management server fails another will step in and act as the primary management server.

Requirements for Single Server Configuration

The following table describes the requirements for Single Server Configuration:

Number of Endpoints	Number of Processors	Clock Speed	Memory	Operating System
1 - 1,000	1 processor	2.8 GHz	1 GB	Windows2003 Server Standard Edition
1,001 – 2,500	1 hyperthreaded processor or 2 processors	2.8 GHz	2 GB	Windows 2003 Server Standard Edition
2,5001 – 5,000	Dual-Core processor	2.8 GHz	2 GB	Windows 2003 Server Enterprise Edition
5,000 – 12,000	2x Dual-Core Processor	3 GHz	4GB	Windows 2003 Server Enterprise Edition

Requirements for Cluster Server Configuration

The following table describes the requirements for Cluster Server Configuration:

Configuration Type	Number of Endpoints	Number of Processors	Clock Speed	Memory	Operating System
Management Server	-	Dual-Core processor	2.8 GHz	2 GB	Windows2003 Server Standard Edition
Regular Server	1 – 1,000	1 processor	2.8 GHz	1 GB	Windows 2003 Server Standard Edition
	1001 – 2,500	1 hyperthreaded processor or 2 processors	2,8 GHz	2 GB	Windows 2003 Server Standard Edition
	2,501 – 5,000	Dual-Core processor	2.8 GHz	2 GB	Windows 2003 Server Enterprise Edition
	5,001 – 12,000	2x Dual-Core Processor	3 GHz	4 GB	Windows 2003 Server Enterprise Edition

Deployment

The installation of the CSS management console and Management servers are wizard driven and uneventful. The agents can be automatically installed on computers in the network, using the Active Directory synchronization feature. For ongoing housekeeping, at intervals the Active Directory and the Central Security Suite database synchronize and agents are automatically being installed on new computers drawn from the Active Directory.

There are four methods of installing and deploying the Agents:

- **Automatic Push** – This is our preferred deployment methodology: Workstation deployment can be handled in two different methods. The first method is an automated push. The automated push can be handled in one of two ways: SMS and Login Script (or preferred distribution solutions). The SMS job will be created for remote deployment of the agents that automatically installs the product without user interaction. A workstation reboot will be required after the installation is completed.

- **Automatic Installation** - Central Security Suite enables automatic installation of agents on computers in the network, using the Active Directory synchronization feature. Once every preset interval, the Active Directory and the Central Security Suite database synchronize and agents are installed on new computers drawn from the Active Directory. This feature allows you to define a time interval during which the synchronization takes place and the necessary action (agent installation). Active Directory synchronization is inactive by default and needs to be configured and started. The configuration is not done via the Management Console.

- **Installation via the Management Console** – Central Security Suite has an independent deployment tool which can be use to install Agents directly from the Console.

- **Manual installation** – Running the Central Security Suite MSI installation file on the machine.

Configurations & Defining Policies

CSS enables administrators to predefine the policy as a part of the automatic deployment of Agents.

Security administrators can manually select and configured the various different levels with layered security policies call ACLs. These policies can then be published to the Agents online.

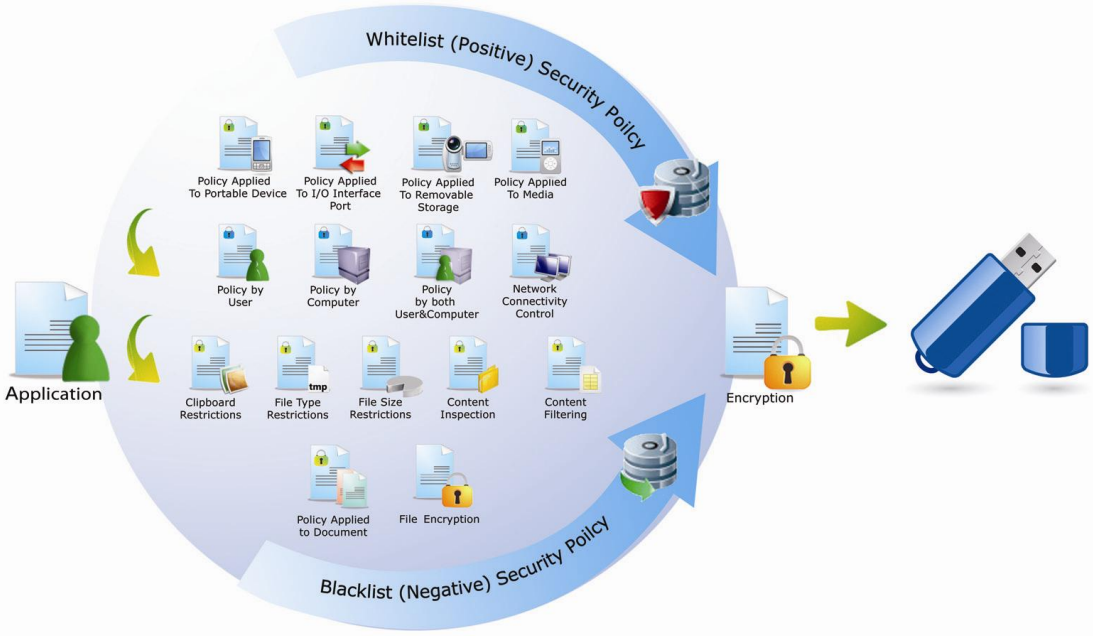
The update of the policies happens in real-time, thus the administrator can stop an action or abuse of a user as needed. The policies offer a great amount of flexibility and granularity across the system.

Policy Granularity

The CSS classifies, identifies and reports on devices by the following parameters:

- Vendor ID (VID) / Device Manufacturer
- Product ID (PID)
- Device Type
- Device Model/Category
- Unique ID
- Unique Serial Number
- Device location: Computer Name and User Name

ControlGuard Information Protection Cycle
Transfer of Information to Removable Storage Devices and Media



Policies of the CSS enterprise can be defined separately for online/offline/VPN policy, internal DNS capabilities, powerful graphical report module and enterprise tuning capabilities.

The VPN, Online and Offline Policy features mean the security applied is adapted dynamically to secure in the appropriate measure whether he user is online, offline or a roaming VPN user.
In addition, the CSS has a feature to support Desktop Virtualization by enforcing a policy on VMware Virtual Desktop without the need of deploying an Agent on the Virtual OS.

Policies can focus on file type, file size, content restriction, content filtering (REGEX), content backup, wireless restrictions by MAC address and SSIDs and print screen.

Data Leakage Prevention (DLP) capabilities of the CSS Enterprise include:

- **File Type Regulation**
  Based on the quick identification of a file by its content and not simply by the file extension

- **File Size Restrictions**
  Limitations can be set for the volume of daily copying limits

- **Content Inspection & Regular Expression Filtering**
  The CSS enterprise provides a powerful regular expression engine that allows blocking content by scanning and identifying prohibited content within documents being copied. This is done by searching out signatures, patterns and strings and preventing the copying of files in which a match is found.

- **Approve Content Policy Bypass**
  When deploying DLP situations may occur where administrators may be hesitant to enact a DLP policy due to exceptions or the administrator may disable a policy in a manner that would allow data loss of other similar documents beyond the one in which the exemption is for. The CSS allows a specific static file to be approved exempt from a DLP policy thus maintaining enforcement of security policies.

- **Print Screen Blocking**
  Prevents the user from obtaining information from creating screen captures using the print screen key.

Blanket policies vs. CSS layered positive and negative (white-lists/blacklists)

The issue of blanket on-size-fits all security policies for endpoints is best illustrated with an example:

In a health insurance company of 800 employees, one would expect to find among the employees titles Claims, Assistant Claims Examiners, Claims

Examiners, Medical Review Staff, Managers, Executives Staff, Accounts Payable, Accounting, Human Resources, etc.

With a one-size fits all policy, flash disks must be allowed for all users in order to let the Management, Accounts Receivable, Medical Review, Claims Examiners, Executive Team and Accountants to take work home. This leaves hundreds of employees with the rights to use USB devices even though they have no work tasks related to removable storage.
Now security must deal unnecessarily monitoring a large number of USB endpoints throughout the company because blocking copy permissions is not granular.

With the CSS ACL (Access Control List) layered approach, white-list and blacklist configurations can be use to block copying of files to USB devices for all users except those given exceptions. The CSS can go even more granular by prohibiting those exempted from using certain types of devices- for example, disallowing a specific brand and model of USB flash disks.

With the CSS, IT security can reduce their workload and the amount of needless monitoring with the ultimate mix of flexible layered ACLs using white list and blacklist policies. The security administrator can assign access and permission to specific users, group of users, specific computer or group of computers for those devices and media that are needed for efficient work. These permissions can be temporary, online/offline and VPN, scheduled, content limit, size limit, read only, read/write, etc.

Events Notifications and Actions

Events include a number of categories, such as configuration events, policy violation events, Agent status, etc. All key events are logged in a variety of logs and if the computer is on the network they will be transmitted to the Management Server.

The CSS provides a number of notification alerts and actions which can be customized.
A security event or violation event can occur when a laptop or PC is connected to the network or when it is disconnected, e.g. when communication with the management server is not possible.

Mortifications can be sent to two locations: the local machine and the Management server which sends them to the management console and the Messaging Console if it is installed.

An alert can be configured to prompt the user and will occur regardless of whether the computer is in the network or not. When an alert is issued and the computer is connected to the network the alert will show in the Management console with information regarding the event.

Alerts can also be configured to be handled by the Messaging Server plug-in.

Events can also trigger automatic actions beyond the security policy restrictions. Actions on the local machine executed by the Agent can include blocking, rebooting the machine, log off the user from the PC, shut down endpoint that the violation occurred on, and custom actions which allow the specification of to locally run a user programmed batch file.

Technology Competitive Edge

The following is a description of some of the many competitive advantages that the ControlGuard CSS product line has over other products that claim to do what we do. ControlGuard is a specialized company focused on securing the portable generation.

Key points to consider:

- Local administrators of the endpoint can remove competitive products' agents. This is an unacceptable attribute for many organizations as it leaves the endpoint security up to the discretion of the end-user. ControlGuard CSS agent is tamper-proof and therefore the end-user cannot bypass, stop, uninstall or interfere in any way with the agent even if they have admin rights to the endpoint.

- With ControlGuard Endpoint Manager, any attempt to use an unauthorized device will generate a real-time notification to the Management Console, where SNMP traps of the Messaging Server add-on can generate an alert to an enterprise management systems and an email will be sent to the security admin (all of the above is configurable). The CSS offer tight integration to specific management systems like CA Security Command Center, CA Audit etc.

- If a PC has a problem and the agent is no longer functional on it, competitive products will leave the administrator uninformed. Since most of the competitor solution allow Task Manager stopping of a process this creates and unnecessary security risk. ControlGuard Management Console displays clearly a network view of all endpoint in the organization and whether or not an agent is not functional.

- The claim of ease of use by many competitors should be scrutinized as many solutions that work well in laboratories are found lacking when deployed and run in real world enterprise scale operations where intelligent organized is a must have. In an enterprise environment with a large number of endpoints, the CSS Management Console displays a clear picture without information overload and displays which endpoints are protected with real-time status and real-time notification. On-line filtering based on endpoint status makes CSS on-going management extremely efficient and simple to use.

- Competitive products lack intelligent and proper approach to endpoint security because they are not specialized. The CSS method of distributing, managing and updating Agents, as well as the layered white-list and blacklist policies, is unrivalled in this sector.

- CSS delivers greater flexibility, granularity, and value by enforcing real-time policies on the endpoints, defining online/offline/VPN policy, internal DNS capabilities, powerful graphical report module and enterprise tuning capabilities.

- CSS offers a wide array of security policy features, which surpasses competitive products, including features targeting files type, file size, content restriction, content filtering, content backup, wireless restrictions by MAC address and SSIDs and print screen.

- CSS ensures that the right security policy is enforced by creating a real-time white-list and blacklist of media and portable devices. CSS

whitelist and blacklist are much more precise, easier to configure and more flexible than competitive products. The real-time mitigation and added security due to its kernel capabilities is what sets the CSS apart. The CSS agents collects information from the devices itself with no dependence what so ever on the machine's registry. This ensures the validity of information such as serial numbers, product IDs, manufacture IDs and specific and unique device IDs. CSS offers greater resistance to false positives events and evasions of smart devices.

Summary

The CSS provides world class endpoint security and an array of features especially catered to the needs of IT security in the real world where real-time security logic and automation features are central to the job of securing companies, systems and the people that depend on them.

If you need more information or have questions regarding the ControlGuard CSS, CSS Add-ons, or any of the ControlGuard products that compliment Endpoint Security, please contact us or visit our website:
www.controlguard.com